**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 4, 2015

*The following cyber advisory was issued by the State of Alaska and
was intended for State government entities. The information may or
may not be applicable to the general public and accordingly, the State
does not warrant its use for any specific purposes.*

ADVISORY NUMBER:
SA2015-020

DATE(S) ISSUED:
03/04/2015

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

EXECUTIVE SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome that could result in remote code
execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities
can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful
exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the
user running the affected application. Depending on the privileges associated with the user, an
attacker could then install programs; view, change, or delete data; or create new accounts with
full user rights.

THREAT INTELLIGENCE:
There is no known proof-of-concept code available at this time.

SYSTEM AFFECTED:
• Google Chrome Prior to 40.0.2272.76

RISK:
Government:
• Large and medium government entities: **High**
• Small government entities: **High**

 Businesses:
• Large and medium business entities: **High**
• Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Multiple Vulnerabilities have been discovered in Google Chrome, and have been patched in the latest Stable Channel Update. This update addressed multiple bug fixes, security updates, and feature enhancements including the following:
- Out-of-bounds write vulnerabilities in Skia filters. [CVE-2015-1213, CVE-2015-1214, CVE-2015-1215]
- Use-after-free vulnerability in v8 bindings. [CVE-2015-1216]
- Security vulnerability exists in v8 because of type. [CVE-2015-1217]
- Use-after-free vulnerability because of DOM error. [CVE-2015-1218]
- Integer-overflow vulnerability due to WebGL error. [CVE-2015-1219]
- Use-after-free vulnerability due GIF decoder error. [CVE-2015-1220]
- Use-after-free vulnerability due to web databases error. [CVE-2015-1221]
- Use-after-free vulnerability due service workers error. [CVE-2015-1222]
- Use-after-free vulnerability due to DOM error. [CVE-2015-1223]
- Security vulnerability due v8 type confusion. [CVE-2015-1230]
- Out-of-bounds read vulnerability due to vpxdecoder error. [CVE-2015-1224]
- Out-of-bounds read vulnerability due to an error in pdfium [CVE-2015-1225]
- Security vulnerability due to debugger validation. [CVE-2015-1226]
- Security vulnerability due to uninitialized value in blink. [CVE-2015-1227]
- Security vulnerability due to uninitialized value in rendering. [CVE-2015-1228]
- Security vulnerability due to proxy-based cookie injection. [CVE-2015-1229]

RECOMMENDATIONS:
We recommend the following actions be taken:
- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Google:
http://googlechromereleases.blogspot.in/2015/03/stable-channel-update.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1213
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1214
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1215
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1216
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1217
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1218
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1219
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1220
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1221
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1222
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1223
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1224
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1225
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1226
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1227
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1228
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1229

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1230